#3

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005-3315

202 • 408 • 4000
FACSIMILE 202 • 408 • 4400

ATLANTA
404•653•6400
PALO ALTO
650•849•6600

WRITER'S DIRECT DIAL NUMBER:

TOKYO
011•813•3431•6943
BRUSSELS
011•322•646•0353

ATTORNEY DOCKET NO. 04329.2191

Assistant Commissioner
for Patents
Washington, D.C. 20231

U.S. Patent Application for
ENCRYPTION APPARATUS, CRYPTOGRAPHIC COMMUNICATION SYSTEM, KEY RECOVERY SYSTEM, AND STORAGE MEDIUM

Inventors: Akito NIWA et al.
Serial No.: 09/448,470 Group Art Unit: 2766
Filed: November 24, 1999

CLAIM FOR PRIORITY

Sir:

Under the provisions of Section 119 of 35 U.S.C., applicants hereby claim the benefit of the filing date of Japanese Patent Application No. 10-334485 filed November 25, 1998, for the above identified United States Patent Application.

In support of applicants' claim for priority, filed herewith is one certified copy of the above.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW
GARRETT & DUNNER, L.L.P

by: _____
Richard V. Burgujian
Reg. No. 31,744

Dated: 1/13/00

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９８年１１月２５日

出 願 番 号
Application Number: 平成１０年特許願第３３４４８５号

出 願 人
Applicant (s): 株式会社東芝

１９９９年１１月２６日

特許庁長官
Commissioner,
Patent Office 近藤隆彦

【書類名】　特許願

【整理番号】　A009805588

【提出日】　平成10年11月25日

【あて先】　特許庁長官　殿

【国際特許分類】　H04L 12/00

【発明の名称】　暗号装置、暗号通信システム及び鍵復元システム並びに記憶媒体

【請求項の数】　6

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　才所　敏明

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　川村　信一

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　堀　智美

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　青木　恵

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　石原　達也

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　佐野　文彦

【発明者】

【住所又は居所】　東京都府中市東芝町１番地　株式会社東芝府中工場内

【氏名】　丹羽　朗人

【特許出願人】

【識別番号】　000003078

【氏名又は名称】　株式会社　東芝

【代理人】

【識別番号】　100058479

【弁理士】

【氏名又は名称】　鈴江　武彦

【電話番号】　03-3502-3181

【選任した代理人】

【識別番号】　100084618

【弁理士】

【氏名又は名称】　村松　貞男

【選任した代理人】

【識別番号】　100068814

【弁理士】

【氏名又は名称】　坪井　淳

【選任した代理人】

【識別番号】　100092196

【弁理士】

【氏名又は名称】　橋本　良郎

【選任した代理人】

【識別番号】　100091351

【弁理士】

【氏名又は名称】　河野　哲

【選任した代理人】

【識別番号】　100088683

【弁理士】

【氏名又は名称】　中村　誠

【選任した代理人】

【識別番号】　100070437

【弁理士】

【氏名又は名称】　河井　将次

【手数料の表示】

【予納台帳番号】　011567

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　暗号装置、暗号通信システム及び鍵復元システム並びに記憶媒体

【特許請求の範囲】

【請求項１】　データ本体を暗号化して送信データに含め、当該送信データを受信者に送信する暗号装置であって、

暗号化したデータ本体を復号する鍵を復元するための復元用情報を、送信者が登録している鍵復元者に復号可能に暗号化した送信者鍵復元データと、

暗号化したデータ本体を復号する鍵を復元するための復元用情報を、受信者が登録している鍵復元者に復号可能に暗号化した受信者鍵復元データと

を前記送信データに含める手段を備えたことを特徴とする暗号装置。

【請求項２】　前記送信者又は前記受信者が複数の鍵復元者に登録している場合に、

前記送信者又は前記受信者鍵復元データに含まれる復元用情報は、暗号化データ本体を復号する復号鍵の部分の集合であり、各復号鍵の部分はそれぞれ異なる鍵復元者に復号可能に暗号化されることを特徴とする請求項１記載の暗号装置。

【請求項３】　前記請求項１又は２記載の暗号装置と、

送信者又は受信者が自己に登録している場合には、その送信者又は受信者鍵復元データを復号可能とする鍵復号者装置と、

少なくとも前記鍵復元者及び前記受信者の認証局登録を受け付け可能に構成されると共に、登録された各受信者が何れの鍵復元者に登録しているかの情報、並びに前記暗号装置が前記復元用情報を鍵復元者に復号可能に暗号化するための情報とを提供可能に構成された認証局装置と

を備えたことを特徴とする暗号通信システム。

【請求項４】　前記鍵復元者に対する登録承認を要求する者に承認を与えると共に、前記送信者又は前記受信者鍵復元データの復号承認を要求する正当権限者に対し、前記送信者又は前記受信者鍵復元データの復号承認を与える承認者装置を備え、

前記鍵復号者装置は、前記承認者の承認を得ている者から依頼された場合にのみ、前記送信者又は前記受信者鍵復元データを復号して返送することを特徴とする請求項３記載の暗号通信システム。

【請求項５】　データを暗号化又は復号するために鍵情報を用いると共に、前記鍵情報を復元するための復元用情報を、自己が登録している鍵復元者に復号可能に暗号化した状態で前記鍵情報と別途に保存する暗号装置と、

前記鍵復元者に対する登録承認を要求する者に承認を与えると共に、暗号化された前記復元用情報の復号承認を要求する正当権限者に対し、前記暗号化された復元用情報の復号承認を与える承認者装置と、

前記承認者の承認を得ている者から復号を依頼された場合にのみ、前記暗号化された復元用情報を復号して返送する鍵復号者装置と

を備えたことを特徴とする鍵復元システム。

【請求項６】　データ本体を暗号化して送信データに含め、当該送信データを受信者に送信する暗号装置を制御するプログラムであって、

暗号化させたデータ本体を復号させる鍵を復元させるための復元用情報を、送信者が登録している鍵復元者に復号可能に暗号化させた送信者鍵復元データと、

暗号化させたデータ本体を復号させる鍵を復元させるための復元用情報を、受信者が登録している鍵復元者に復号可能に暗号化させた受信者鍵復元データと

を前記送信データに含めさせる手段を有するプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は暗号及び復号処理に用いる暗号鍵及び復号鍵の管理の部分に特徴のある暗号装置、暗号通信システム及び鍵復元システム並びに記憶媒体に関するものである。

【０００２】

【従来の技術】

近年では、オープンなネットワーク上でデータ（メッセージ）通信を行う場合、データの盗聴及び改竄を防止するためにデータを暗号化するようになっている。

【０００３】

このデータ暗号化のために暗号鍵が用いられるが、ユーザ自身による鍵の紛失や何らかの原因により鍵を破壊してしまう場合がある。また、状況に応じて正当な理由を持つ第三者が、暗号通信を傍受する必要性が生じる場合もある。これらの事態に対応するために、何らかの方式で鍵を復元できることが要求される。

【０００４】

従来、提供されている鍵復元システムは、暗号通信の当事者が鍵復元処理を実際に行う鍵復元エージェントに予め登録をしておき、その登録に対応して復号可能とした鍵復元フィールドを暗号化データに付加することで実現される。この鍵復元フィールドは暗号化されているが、これを復号することで当該鍵（通信用の共通鍵等）が復元されるようになっている。

【０００５】

すなわち、送受信者や正当権限を有する第三者は必要な場合には鍵復元フィールドを鍵復元エージェントに送信し、紛失等した鍵を復元してもらうようになっている。

【０００６】

【発明が解決しようとする課題】

しかしながら、上記した従来の鍵復元方式では、鍵復元エージェントにとって鍵の復元要求者が正当な権限を有しているか否かを確認することが困難である。また、鍵復元エージェントが悪意の第三者と結託して不正な鍵復元を行うような場合を防止することはできない。

【０００７】

さらに、データ通信における送信者と受信者とが異なる鍵復元エージェントに登録しているような場合、特に国際間における暗号通信の場合には、受信者

や正当権限第三者が登録している鍵復元エージェントでは送信者の鍵復元フィールドを復元することができない。例えば送信者がＡという鍵復元エージェントに登録し、受信者がＢという鍵復元エージェントに登録しており、受信者はＡの存在がわからないような場合を考える。このとき、受信者が例えば暗号通信用の共通鍵を紛失すると、暗号化データの鍵復元フィールドをＢに送っても紛失した共通鍵は復元できない。また、送信者と受信者が異なる国の者であるような場合には、受信者はＡの所在を知ることは容易ではない。正当権限第三者についても同様な事情が生じる。

【０００８】

本発明は、このような実情を考慮してなされたもので、その第１の目的は、鍵復号に関する権限集中やエージェントの結託等の防止を可能として、鍵復元の安全性を高いものとすることができる暗号通信システム及び鍵復元システムを提供することにある。

【０００９】

また、第２の目的は、異なるエージェントに登録するユーザ間で暗号化通信を行う場合でも、そのユーザあるいは正当権限を有する第三者が容易にエージェント情報を取得でき、鍵復元を行うことができる暗号装置、暗号通信システム及び鍵復元システム並びに記憶媒体を提供することにある。

【００１０】

【課題を解決するための手段】

上記課題を解決するために、請求項１に対応する発明は、データ本体を暗号化して送信データに含め、当該送信データを受信者に送信する暗号装置であって、暗号化したデータ本体を復号する鍵を復元するための復元用情報を、送信者が登録している鍵復元者に復号可能に暗号化した送信者鍵復元データと、暗号化したデータ本体を復号する鍵を復元するための復元用情報を、受信者が登録している鍵復元者に復号可能に暗号化した受信者鍵復元データとを送信データに含める手段を備えた暗号装置である。

【００１１】

本発明はこのような手段を設けたので、それぞれ異なる鍵復元者に登録する

送受信者間で暗号化通信を行う場合でも、その送受信者あるいは正当権限を有する第三者が容易に鍵復元を行うことができる。

【００１２】

次に、請求項２に対応する発明は、請求項１に対応する発明において、送信者又は受信者が複数の鍵復元者に登録している場合に、送信者又は受信者鍵復元データに含まれる復元用情報は、暗号化データ本体を復号する復号鍵の部分の集合であり、各復号鍵の部分はそれぞれ異なる鍵復元者に復号可能に暗号化される暗号装置である。

【００１３】

本発明はこのような手段を設けたので、鍵を復元するための情報の復号を、複数の鍵復元者に分散させて行わせることができ、鍵情報の秘匿安全性を高めることができる。

【００１４】

次に、請求項３に対応する発明は、請求項１又は２に対応する暗号装置と、送信者又は受信者が自己に登録している場合には、その送信者又は受信者鍵復元データを復号可能とする鍵復号者装置と、少なくとも鍵復元者及び受信者の認証局登録を受け付け可能に構成されると共に、登録された各受信者が何れの鍵復元者に登録しているかの情報、並びに前記暗号装置が復元用情報を鍵復元者に復号可能に暗号化するための情報とを提供可能に構成された認証局装置とを備えた暗号通信システムである。

【００１５】

本発明はこのような手段を設けたので、それぞれ異なる鍵復元者に登録する送受信者間で暗号化通信を行う場合でも、その送受信者あるいは正当権限を有する第三者が容易に鍵復元者についての情報を取得することができ、かつ容易に鍵復元を行うことができる。さらに、鍵復号に関する権限集中や鍵復元者と悪意の者との結託等の防止を可能として、鍵復元の安全性を高いものとすることができる。

【００１６】

次に、請求項４に対応する発明は、請求項３に対応する発明において、鍵復

元者に対する登録承認を要求する者に承認を与えると共に、送信者又は受信者鍵復元データの復号承認を要求する正当権限者に対し、送信者又は受信者鍵復元データの復号承認を与える承認者装置を備え、鍵復号者装置は、承認者の承認を得ている者から依頼された場合にのみ、送信者又は受信者鍵復元データを復号して返送する暗号通信システムである。

【００１７】

本発明はこのような手段を設けたので、鍵復元者と悪意の者との結託等の防止が一層強化され、鍵復元の安全性をより高いものとすることができる。

【００１８】

次に、請求項５に対応する発明は、データを暗号化又は復号するために鍵情報を用いると共に、鍵情報を復元するための復元用情報を、自己が登録している鍵復元者に復号可能に暗号化した状態で鍵情報と別途に保存する暗号装置と、鍵復元者に対する登録承認を要求する者に承認を与えると共に、暗号化された復元用情報の復号承認を要求する正当権限者に対し、暗号化された復元用情報の復号承認を与える承認者装置と、承認者の承認を得ている者から復号を依頼された場合にのみ、暗号化された復元用情報を復号して返送する鍵復号者装置とを備えた鍵復元システムである。

【００１９】

本発明はこのような手段を設けたので、あらゆる種類の鍵情報の復元を可能とすると共に、鍵復号に関する権限集中や鍵復元者と悪意の者との結託等の防止を可能として、鍵復元の安全性を高いものとすることができる。

【００２０】

次に、請求項６に対応する発明は、請求項１に対応する発明をコンピュータに実現させるプログラムを記憶した記憶媒体である。

【００２１】

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項１の暗号装置として機能する。

【００２２】

【発明の実施の形態】

以下、本発明の実施の形態について説明する。

【００２３】

図１は本発明の実施の形態に係る暗号通信システムの全体構成例を示す構成図である。

【００２４】

この暗号通信システムは、ユーザ１間で暗号化通信を行う場合に、そのセッション鍵やユーザ秘密鍵を復元可能とするために、鍵復元エージェント３，認証局２及び承認者４を設けてなるものである。ユーザ１，鍵復元エージェント３，認証局２及び承認者４の間は公衆回線等からなるネットワーク（インターネット等）で通信可能に構成されている。

【００２５】

図２は本実施形態のユーザ１，鍵復元エージェント３，認証局２（鍵復元センタ）又は承認者４を構成する装置のハードウエア構成例を示すブロック図である。

【００２６】

ユーザ１，鍵復元エージェント３，認証局２又は承認者４を構成する装置１１は、ハードウエア的には、ＣＰＵ１２、コントローラ１３、メモリ１４、通信デバイス１５、ディスプレイ１６、キーボード１７、プリンタ１８及びデータバス１９より構成される計算機システムである。

【００２７】

これらの構成のうち、メモリ１４は、いわゆる主記憶（ＲＡＭ等）と二次記憶装置（ハードディスク等）の双方を含むものである。この主記憶上に読み込まれたプログラムと、このプログラムに従うＣＰＵ１２の制御によって、ユーザ１，鍵復元エージェント３，認証局２又は承認者４が行うべき機能が実現される。すなわちソフトウエア的には、ユーザ１，鍵復元エージェント３，認証局２又は承認者４は異なる構成を有するのものである。これらハードウエア及びソフトウエアの結合からなるそれぞれの機能の詳細な内容については、後述する動作説明において流れ図により説明する。

【００２８】

また、メモリ１４の二次記憶装置の部分には、ユーザ１，鍵復元エージェント３，認証局２又は承認者４それぞれに対応して、通信メッセージや各種証明書、公開鍵、各種情報リスト等が格納され、各機能の実現に際して使用される。

【００２９】

さらに、通信デバイス１５は、ネットワークに接続され、ＣＰＵ１２の制御によって、各種の情報を送受する。

【００３０】

次に、ユーザ１，鍵復元エージェント３，認証局２又は承認者４について説明する。

【００３１】

ユーザ１は、暗号メッセージ（暗号通信）の送信者、受信者あるいは当該暗号メッセージを傍受する正当権限を有する第三者を示している。図１では、ユーザ１（＃１）を送信者、ユーザ１（＃２）を受信者、ユーザ１（＃３）を正当権限第三者としている。また、ユーザ１は、送信者、受信者及び正当権限第三者に必要な全ての機能を備えており、状況によって、これらの何れかになる。

【００３２】

具体的には、ユーザ１は、自己の公開鍵、秘密鍵を有すると共に、鍵復元エージェント３の登録機能、暗号メッセージ作成機能、メッセージ送受信機能、暗号メッセージ復号機能及び鍵の復元要求・復元機能等を備えている。なお、図２の装置１１は、ユーザ１の暗号装置を構成するものである。

【００３３】

鍵復元エージェント３は、自己の公開鍵と秘密鍵を有し、登録されたユーザ１からの要求に応じ、受信した鍵復元フィールドを自己の秘密鍵で復号して返信するものである。これらの処理を行うに際し、登録時の承認者４の署名を確認するようになっている。また、鍵復元エージェント３は、多数存在することが可能で、認証局２への登録により、ある者は本実施形態でいう鍵復元エージェント３となる。本実施形態では、鍵復元エージェント３（＃１）～３（＃ｎ

）が存在する。

【００３４】

認証局２は、自己の公開鍵及び秘密鍵を有すると共に、各ユーザ１、各鍵復元エージェント３、各承認者４についての公開鍵に署名（認証）を与え、各種の証明書を発行すると共に、これらの情報をユーザ１等に開放するものである。

【００３５】

承認者４は、ユーザ１が鍵復元エージェントに登録したり鍵復元要求を行う場合等に当該ユーザ１に承認書を発行するものである。この承認者４も多数存在することが可能であり、本実施形態では、承認者４（＃１）～４（＃ｍ）が存在する。なお、ユーザ１が複数の承認者４から１つの承認をもらうことも可能であり、このような場合には、代表承認者が設けられる。

【００３６】

次に、以上のように構成された本実施形態における暗号通信システム及び暗号装置の動作について説明する。

【００３７】

この暗号通信システムにおいては、まず鍵復元エージェントが認証局に自己の公開鍵を登録し、鍵復元を望むユーザは、認証局に登録された何れかの鍵復元エージェントから鍵復元要求を行うエージェントを選択して予め登録する。

【００３８】

このような準備の後、ユーザ間通信が行われ、鍵紛失等により通信用のセッション鍵やユーザ秘密鍵を復元する必要があるときには、登録したエージェントに鍵復元を依頼する。

【００３９】

以下、本システムの動作について、登録、通信及び鍵復元のそれぞれについて説明する。

（鍵復元エージェントの登録手続き）

図３は鍵復元エージェントの認証局への登録手続処理を示す流れ図である。

【００４０】

まず、認証局２への登録を望む鍵復元エージェント３は、自己の公開鍵と公開鍵に対する自分の署名を含む登録申請書を認証局２へ送信する（図３：ｓ１，図１：ａ）。

【００４１】

認証局２はこの鍵復元エージェント３についての調査や署名確認等を行った後（図３：ｓ２）、当該鍵復元エージェント３に対し、鍵復元エージェント３の公開鍵を含む申請データに認証局の署名を付加した公開鍵証明書１７を発行する（図３：ｓ３，図１：ｂ）。

【００４２】

こうして登録された鍵復元エージェント３については、認証局２にてユーザ／承認者／鍵復元エージェントの登録情報テーブルに登録され、この登録情報テーブルの内容はユーザ１等に開放される。以下、鍵復元エージェント３というときは、認証局２に登録されたエージェントを意味する。

（ユーザの登録手続き）

次に、メッセージ通信を行いたいユーザ１は、鍵復元エージェントを選択し、自己が何れの鍵復元エージェント３を利用するかについて、認証局２に登録を行う。

【００４３】

図４はユーザの鍵登録エージェント登録手続処理を示す流れ図である。

【００４４】

ここでは図１のユーザ１（＃１）が登録を行う場合について説明する。

【００４５】

まず、ユーザ１（＃１）は、一又は複数の鍵復元エージェント３への加入に際し、まず承認者４に対し、鍵復元エージェント登録申請１８を行う（図４：ｔ１，図１：ｃ）。

【００４６】

ユーザ１は、一の承認者４に対して承認を求めるようにしてもよいが、鍵復元に関する安全性を高めるために複数の承認者４に承認を求めるようにしてもよい。複数の承認者４に承認を求める場合には、ユーザ１は代表承認者のみに

登録申請を行う（図４：ｔ１）。

【００４７】

代表承認者は各承認者４に登録申請書を回付し、各承認者４は鍵復元エージェント登録申請内容を検査し署名を施す（例えば、多重署名方式を用いる）。申請書は、最後に代表承認者に戻され、当該代表承認者からユーザ１（＃１）に鍵復元エージェント登録承認書が送信される（図４：ｔ２，図１：ｄ）。

【００４８】

次に、ユーザ１（＃１）は自己が登録を希望する各鍵復元エージェント３に対し、承認者４から取得した鍵復元エージェント登録承認書を添付して加入申請を行う（図４：ｔ３，図１：ｅ）。なお、ユーザ１が登録する鍵復元エージェント３は、一つでもよいが、本実施形態では原則として複数の鍵復元エージェント３に登録する場合で説明する。

【００４９】

登録承認書を受けた各鍵復元エージェント３は鍵復元エージェント登録承認書における承認者４の署名を検証し、自身の署名を付加し、ユーザ１（＃１）に対し鍵復元エージェント登録証明書を発行する（図４：ｔ４，図１：ｆ）。

【００５０】

次に、全ての鍵復元エージェント３について鍵復元エージェント登録証明書の取得処理が終了していなければ、ステップｔ１～ｔ４の処理を繰り返す（図４：ｔ５）。

【００５１】

次に、ユーザ１（＃１）は認証局２に対し、エージェント３から取得した鍵復元エージェント登録証明書を添付して登録鍵復元エージェントリスト証明書の発行申請を行う（図４：ｔ６，図１：ｇ）。

【００５２】

認証局２はこの鍵復元エージェント登録証明書における鍵復元エージェント４による署名を検証し、自身の署名を付加し、ユーザ１（＃１）に対し登録鍵復元エージェントリスト証明書を発行する（図４：ｔ７，図１：ｈ）。

【００５３】

このエージェントリストにリストアップされた鍵復元エージェント３がユーザ１（＃１）の登録鍵復元エージェント３であり、ユーザ１（＃１）用の鍵復元フィールドは、これらのエージェント３の有する秘密鍵で解読可能となる。

【００５４】

なお、認証局２は、登録鍵復元エージェントリスト証明書を発行すると共に、同リストの内容を上記登録情報テーブルに反映させる。

【００５５】

図５は認証局に設けられた登録情報テーブルの構成例を示す図である。

【００５６】

同図に示すように、登録情報テーブル２１には、ユーザ１，承認者４又は鍵復元エージェント３のユーザＩＤ（識別情報）２２に対応して、認証局がその者の公開鍵として認証した署名付き公開鍵２３と、ユーザ登録エージェントリスト２４とが設けられている。

【００５７】

署名付き公開鍵２３は、その鍵が当該ユーザ１等の公開鍵であることを認証局が証明するものであり、公開鍵証明書の形で当該情報の要求者に発行される。

【００５８】

ユーザ登録エージェントリスト２４は、各登録ユーザのみに対応して設けられ、このリスト内容の発行を受けることで、第三者は当該ユーザ１がどの鍵復元エージェント３に登録しているかを知ることができる。

【００５９】

なお、この登録情報テーブル２１の内容は一般に公開されており、ユーザ１やエージェント３等はあたかも電話帳を調べるような形でその内容を知ることができる。また、テーブル２１に登録されたエージェント３は、自己の公開鍵を認証局２に登録しており、これらの公開鍵はテーブル２１上に掲載してもよい。

（暗号化メッセージの送受信処理）

次に、このようなエージェント登録を行ったユーザ１間で、実際に暗号化メ

ッセージを送受信するときの処理を説明する。なお、この場合は、ユーザ１（＃１）が送信者となり、ユーザ１（＃２）が受信者となる場合を説明する。ユーザ１（＃２）も図４に示す処理によりエージェント登録を行っているものとする。

【００６０】

図６は暗号化メッセージの送受信処理を示す流れ図である。

【００６１】

図７は暗号化メッセージの送受信を行う場合のユーザ及び認証局の関係を示す図である。

【００６２】

まず、送信者であるユーザ１（＃１）（以下、単に送信者ともいう）は、受信者であるユーザ１（＃２）（以下、単に受信者ともいう）が登録している鍵復元エージェント３の情報を得るために、認証局２へ受信者の公開鍵と登録鍵復元エージェントリストの照会を行う（図６：ｖ１，図７：ｉ）。

【００６３】

認証局２は、登録情報テーブル２１の内容から受信者の公開鍵証明書と登録鍵復元エージェントリスト証明書を作成し、送信者に送信する（図６：ｖ２，図７：ｊ）。この処理は、ユーザ１が認証局２に設けられた電話帳（登録情報テーブル２１）を調べる行為に相当する。

【００６４】

次に、送信者は、認証局２から入手した受信者の登録鍵復元エージェントリスト証明書を利用して送信メッセージ（暗号化メッセージ）を作成する（図６：ｖ３）。

【００６５】

図８は送信者が作成する暗号化メッセージのデータ構造例を示す図である。

【００６６】

この暗号化メッセージ３１は、ヘッダ３２と、送信側鍵復元フィールド３３と、受信側鍵復元フィールド３４と、署名３５と、セッション鍵配送情報３６と、暗号化メッセージ本体３７とから構成される。

【００６７】

ここでまずヘッダ３２には、送信側及び受信側鍵復元フィールド等の後続するデータのサイズ等の情報が格納される。

【００６８】

送信側鍵復元フィールド３３には、送信者側の鍵復元エージェント３が鍵を復元する際に用いる情報が格納され、受信側鍵復元フィールド３４には、受信者側の鍵復元エージェント３が鍵を復元する際に用いる情報が格納される。送信側及び受信側鍵復元フィールド３３，３４には、鍵復元エージェント３のＩＤ３８と、鍵復元エージェント３の公開鍵で暗号化したセッション鍵又はセッション鍵ピース［［Ｓｋｉ］ＫＲＡ（ｉ）ｐｂ］のデータ３９との組が鍵復元エージェント数だけ格納される。

【００６９】

なお、受信側鍵復元フィールド３４を作成するために用いる受信者のエージェントＩＤ及びエージェント公開鍵は、ステップｖ２で入手した登録鍵復元エージェントリスト証明書から取得する。

【００７０】

また、暗号化メッセージ３１には、送信側及び受信側鍵復元フィールド［ＫＲＦ］３３，３４の改竄防止のために、送信者の鍵［ＵＳＲ１ｐｒ］を用いて生成した署名３５（［［ＫＲＦ］ＵＳＲ１ｐｒ］）が付加されている。

【００７１】

セッション鍵配送情報３６には、受信者の公開鍵［ＵＳＲ２ｐｂ］で暗号化したセッション鍵［［ＳＫ］ＵＳＲ２ｐｂ］が格納される。

【００７２】

暗号化メッセージ３１の最後には、送信データの本体として、セッション鍵［ＳＫ］で暗号化した暗号化メッセージ本体３７（［［Ｍ］ＳＫ］）が付加されている。

【００７３】

さて、このように構成された暗号化メッセージ３１は、送信者（ユーザ１（＃１））から受信者（ユーザ１（＃２））に送信される（図６：ｖ４，図７：

ｋ）。

【００７４】

受信者は、図８に示す構造の暗号化メッセージを受け取ると、自己の秘密鍵を用いてセッション鍵情報３６を復号してセッション鍵を取り出し、さらに、そのセッション鍵を用いて暗号化メッセージ本体３７を復号して送信データを取り出す（図６：ｖ５）。

（セッション鍵の鍵復元手続き）

上記図６のステップｖ５のように正常に暗号化メッセージを復号できた場合には特に問題は生じない。ここでは、ユーザ１がセッション鍵を紛失したような場合の復元処理について説明する。

【００７５】

図９は送信者又は受信者による鍵復元手続処理を示す流れ図である。

【００７６】

図１０は送信者又は受信者による鍵復元手続のユーザ，鍵復元エージェント及び承認者の関係を示す図である。

【００７７】

ここではまず、鍵復元を依頼するユーザ１が、復元対象となる鍵復元フィールドを復元可能な鍵復元エージェント３に関する情報（ＩＤ等）を予め有している場合について説明する。このような場合は、ユーザ１がメッセージの送信者（ユーザ１（＃１））である場合や受信者（ユーザ１（＃２））である場合である。

【００７８】

ここでは、受信者がセッション鍵を何らかの理由で取得できなくなり、暗号化メッセージ本体３７を読めなくなってしまった場合について説明する。

【００７９】

ユーザ１（＃２）は、セッション鍵を紛失等した場合（図９：ｗ１）、まず、承認者４に対し鍵復元承認申請書を送信する（図９：ｗ２，図１０：１）。

【００８０】

承認者４は鍵復元承認申請書を検査した後、署名を施し（例えば、多重署名

方式を用いる）、代表承認者から鍵復元承認書をユーザ１（＃２）へ送信する（図９：ｗ３，図１０：ｍ）。

【００８１】

次に、ユーザ１（＃２）は、暗号化メッセージ３２から鍵復元フィールド３３又は３４を取り出し、鍵復元フィールドに指定されている各鍵復元エージェント３へ対するメッセージを作成する（図９：ｗ４）。

【００８２】

図１１はユーザが鍵復元エージェントに送信するメッセージのデータ構造例を示す図である。

【００８３】

同図に示すように、このメッセージ４１は、承認者４から得た鍵復元承認書４２と、暗号化メッセージ３１から取り出した鍵復元フィールド４３と、復元したセッション鍵ピースを送信する際に用いる暗号鍵４４とから構成されるデータ［M′］を、各鍵復元エージェントの公開鍵［ＫＲＡ（ｉ）ｐｂ］で暗号化してなるものである。

【００８４】

ユーザ１（＃２）は、承認書４２及び復元フィールド４３を含むこのメッセージ４１を各鍵復元エージェント３に送信する（図９：ｗ５，図１０：ｎ）。

【００８５】

鍵復元エージェント３は暗号化された［［M′］ＫＲＡ（ｉ）ｐｂ］４１′を自己の秘密鍵で復号して鍵復元承認書、鍵復元フィールド及び暗号鍵［ＳＫ′］を取り出し、鍵復元承認書４２における承認者の署名を検証する（図９：ｗ６）。

【００８６】

承認書４２の確認の後、鍵復元エージェント３は、鍵復元フィールド４３を自己の秘密鍵で復号し、セッション鍵のピースを復元する（図９：ｗ７）。この復元したピースは、暗号鍵［ＳＫ′］４４で暗号化され、エージェント３からユーザ１（＃２）へ送信される（図９：ｗ７，図１０：ｏ）。

【００８７】

このセッションピースを受け取ったユーザ１（＃２）は、各鍵復元エージェント３から送信された暗号化されたセッション鍵のピースを暗号鍵［ＳＫ′］４４で復号する。さらに、例えばラグランジュ補間多項式を用い、復号されたセッション鍵のピースをもとに元のセッション鍵を復元する（図９：ｗ７）。

【００８８】

なお、ラグランジュ補間多項式を用いるのは、複数のピースのうち一定数以上のピースが復元できれば、セッション鍵を復元できるようにするためである。つまり、ラグランジェ補間多項式を用いて鍵をピースに分散した場合、ｎ個に分散した鍵ピースから所定のｋ（＜＝ｎ）個だけ集めるだけで鍵を復元できるものである。

【００８９】

次に、鍵復元を依頼するユーザ１が、復元対象となる鍵復元フィールドを復元可能な鍵復元エージェント３に関する情報（ＩＤ等）を有していない場合について説明する。このような場合は、ユーザ１が正当権限を有する第三者（ユーザ１（＃１））のような場合が考えられる。

【００９０】

図１２は第三者による鍵復元手続処理を示す流れ図である。

【００９１】

この場合には、まず、暗号化メッセージ３１に含まれる鍵復元フィールド３３又は３４についての鍵復元エージェント３の情報を取得する必要がある。

【００９２】

このためにまず、ユーザ１（＃３）は認証局２へ送信者又は受信者の公開鍵と登録鍵復元エージェントリストの照会を行う（図１２：ｘ１）。

【００９３】

認証局２は、登録情報テーブル２１の内容から送信者又は受信者の公開鍵証明書と登録鍵復元エージェントリスト証明書を作成しユーザ１に送信し、ユーザ１（＃３）はこれを受信する（図１２：ｘ２）。この処理は、ユーザ１（＃３）が認証局２に設けられた電話帳（登録情報テーブル２１）を調べる行為に相当する。

【００９４】

以下、ユーザ１（＃３）は、承認者４に鍵復元のための承認を求め（図１：ｐ，ｑ）、その承認書を復号対象の鍵復元フィールドとともに鍵復元エージェント３に送付して復元ピースを受領し（図１：ｒ，ｓ）、さらにはセッション鍵を復元することになる。この処理は図１１のステップｗｗ（ｗ２～ｗ８）と同様であるので詳細説明は省略する。

（他の鍵の鍵復元手続き）

上記場合は、暗号通信に含まれるセッション鍵そのものの復元について説明したが、本実施形態のシステムを用いれば他の鍵の復元も可能である。この他の鍵として、ユーザ１等が用いる秘密鍵（ユーザ秘密鍵）の場合でその復元処理を説明する。なお、この場合には、本実施形態は、鍵復元システムとして動作する。

【００９５】

図１３は鍵復元手続におけるユーザ，鍵復元エージェント及び承認者の関係を示す図である。

【００９６】

ユーザ１（＃１）は、自身の秘密鍵を鍵復元エージェント３の公開鍵で暗号化（登録エージェントが一つの場合）、または秘密鍵をピースに分割し（登録エージェントが複数の場合、以下この場合で説明する）、各々のピースに対し異なる鍵復元エージェント３の公開鍵で暗号化したユーザ秘密鍵復元フィールドを生成し、秘密鍵のバックアップとしてユーザが所有する記憶装置に保存しておく。このユーザ秘密鍵復元フィールドは、図８における送信側又は受信側鍵復元フィールドに相当する。

【００９７】

ユーザ秘密鍵復元フィールドには、鍵復元エージェントのＩＤと鍵復元エージェントの公開鍵で暗号化した秘密鍵又は暗号化した秘密鍵ピースのデータが鍵復元エージェント数だけ格納されている。秘密鍵が何らかの原因で紛失または破壊され、ユーザ自身で復元できなくなった場合に、ユーザ１（＃１）は承認者４に対しユーザ秘密鍵復元承認申請を行う（図１３：ｔ）。各承認者４は

ユーザ秘密鍵復元承認申請を検査し署名を施し（例えば多重署名を用いる）、最後の承認者（代表承認者）からユーザ秘密鍵復元承認書をユーザ１（＃１）に送信する（図１３：ｕ）。

【００９８】

次に、ユーザ１（＃１）は各鍵復元エージェント３へ、各鍵復元エージェントの公開鍵で暗号化したユーザ秘密鍵復元承認書、ユーザ秘密鍵復元フィールド及び復元したユーザ秘密鍵またはユーザ秘密鍵ピースを送信する際に用いる暗号鍵を送信する（図１３：ｖ）。このとき送信するデータは図１１に示すものと同様なものである。

【００９９】

各鍵復元エージェント３は、暗号化されたユーザ秘密鍵復元承認書、ユーザ秘密鍵復元フィールド及び復元したユーザ秘密鍵ピース（又はユーザ秘密鍵）を送信する際に用いる暗号鍵を復号し、ユーザ秘密鍵復元承認書における承認者の署名検証する。その後、ユーザ秘密鍵復元フィールドを用いて各々の鍵復元エージェントが秘密鍵のピース（又は秘密鍵全体）を復元し、ユーザが指定した秘密鍵ピース送信用の暗号鍵を用いて暗号化した秘密鍵ピース（又は秘密鍵全体）をユーザ１（＃１）に送信する（図１３：ｗ）。

【０１００】

ユーザ１（＃１）は、各鍵復元エージェント３から送信された暗号化された秘密鍵ピース（又は秘密鍵全体）を復号する。また、ピースを受け取った場合には、例えばラグランジュ補間多項式を用い、秘密鍵のピースに基づき元の秘密鍵を復元する。

【０１０１】

上述したように、本発明の実施の形態に係る暗号通信システム及び暗号装置は、鍵復元エージェント３の他、認証局２及び承認者４を設けるようにしたので、鍵復元エージェントの鍵復元に対する権力を分散化することができ、鍵復元の安全性を高いものとすることができる。

【０１０２】

また、鍵復元センター（認証局）や鍵復元エージェントによる鍵復元機能の

集中化を抑制するために、少なくとも一人以上で構成される承認者が、鍵復元エージェントに対するユーザ登録申請書、鍵復元申請書、秘密鍵復元申請書を検証及び承認するので、各種情報を管理する認証局２の他に、第三者的な承認者４による承認処理が導入され、鍵復元に関する安全性は特に高いものとなる。

【０１０３】

さらに、ユーザは、認証局に登録された複数の鍵復元エージェントから適宜選択しエージェント登録を行うことができるので、一層安全性、信頼性の高い鍵復元を実施することができる。また、鍵復元エージェントの悪意の者との結託等も防止できる。

【０１０４】

また、認証局２に登録情報テーブル２１を設けてその情報を一般に開放するようにしたので、エージェントへの登録情報等を問い合わせることが容易であり、異なる鍵復元エージェント３に登録するユーザ間の暗号通信における鍵復元処理の容易に行うことができる。

【０１０５】

さらに、送信者が登録する鍵復元エージェントの情報が含まれている送信側鍵復元フィールドと、受信者が登録する鍵復元エージェントの情報が含まれている受信側鍵復元フィールドを生成し、暗号化データと共に送信するようにしたので、データ通信を行う送信者と受信者が異なる鍵復元センターの管轄下にある場合であっても鍵復元を容易に行うことができる。

【０１０６】

また、本実施形態の鍵復元システムによれば、暗号化データを生成する際に用いるセッション鍵の復元だけでなく、鍵配送や署名生成等に用いる秘密鍵についてもその鍵情報を複数の鍵復元エージェントを用いて復元することができる。

【０１０７】

なお、本発明は、記憶媒体に格納したプログラムやデータ等をコンピュータに読み込ませて実現することが可能であり、この記憶媒体としては、磁気ディ

スク、フロッピーディスク、ハードディスク、光ディスク（ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＤＶＤ等）、光磁気ディスク（ＭＯ等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であってもよい。

【０１０８】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているＯＳ（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のＭＷ（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行してもよい。

【０１０９】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、ＬＡＮやインターネット等により伝送されたプログラムをダウンロードして記憶又は一時記憶した記憶媒体も含まれる。

【０１１０】

また、記憶媒体は１つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何らの構成であってもよい。

【０１１１】

なお、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の１つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であってもよい。

【０１１２】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【０１１３】

【発明の効果】

以上詳記したように本発明によれば、鍵復号に関する権限集中やエージェン

トの結託等の防止を可能として、鍵復元の安全性を高いものとすることができる暗号通信システム及び鍵復元システムを提供することができる。

【０１１４】

また、本発明によれば、異なるエージェントに登録するユーザ間で暗号化通信を行う場合でも、そのユーザあるいは正当権限を有する第三者が容易にエージェント情報を取得でき、鍵復元を行うことができる暗号装置、暗号通信システム及び鍵復元システム並びに記憶媒体を提供することができる。

【図面の簡単な説明】

【図１】

本発明の実施の形態に係る暗号通信システムの全体構成例を示す構成図。

【図２】

同実施形態のユーザ，復元エージェント，認証局又は承認者を構成する装置のハードウエア構成例を示すブロック図。

【図３】

鍵復元エージェントの認証局への登録手続処理を示す流れ図。

【図４】

ユーザの鍵登録エージェント登録手続処理を示す流れ図。

【図５】

認証局に設けられた登録情報テーブルの構成例を示す図。

【図６】

暗号化メッセージの送受信処理を示す流れ図。

【図７】

暗号化メッセージの送受信を行う場合のユーザ及び認証局の関係を示す図。

【図８】

送信者が作成する暗号化メッセージのデータ構造例を示す図。

【図９】

送信者又は受信者による鍵復元手続処理を示す流れ図。

【図１０】

送信者又は受信者による鍵復元手続のユーザ，鍵復元エージェント及び承認

者の関係を示す図。

【図１１】

ユーザが鍵復元エージェントに送信するメッセージのデータ構造例を示す図。

【図１２】

第三者による鍵復元手続処理を示す流れ図。

【図１３】

鍵復元手続におけるユーザ，鍵復元エージェント及び承認者の関係を示す図。

【符号の説明】

１…ユーザ

２…鍵復元エージェント

３…認証局

４…承認者

１１…鍵復元エージェント，認証局又は承認者を構成する装置

１２…ＣＰＵ

１３…コントローラ

１４…メモリ

１５…通信デバイス

１６…ディスプレイ

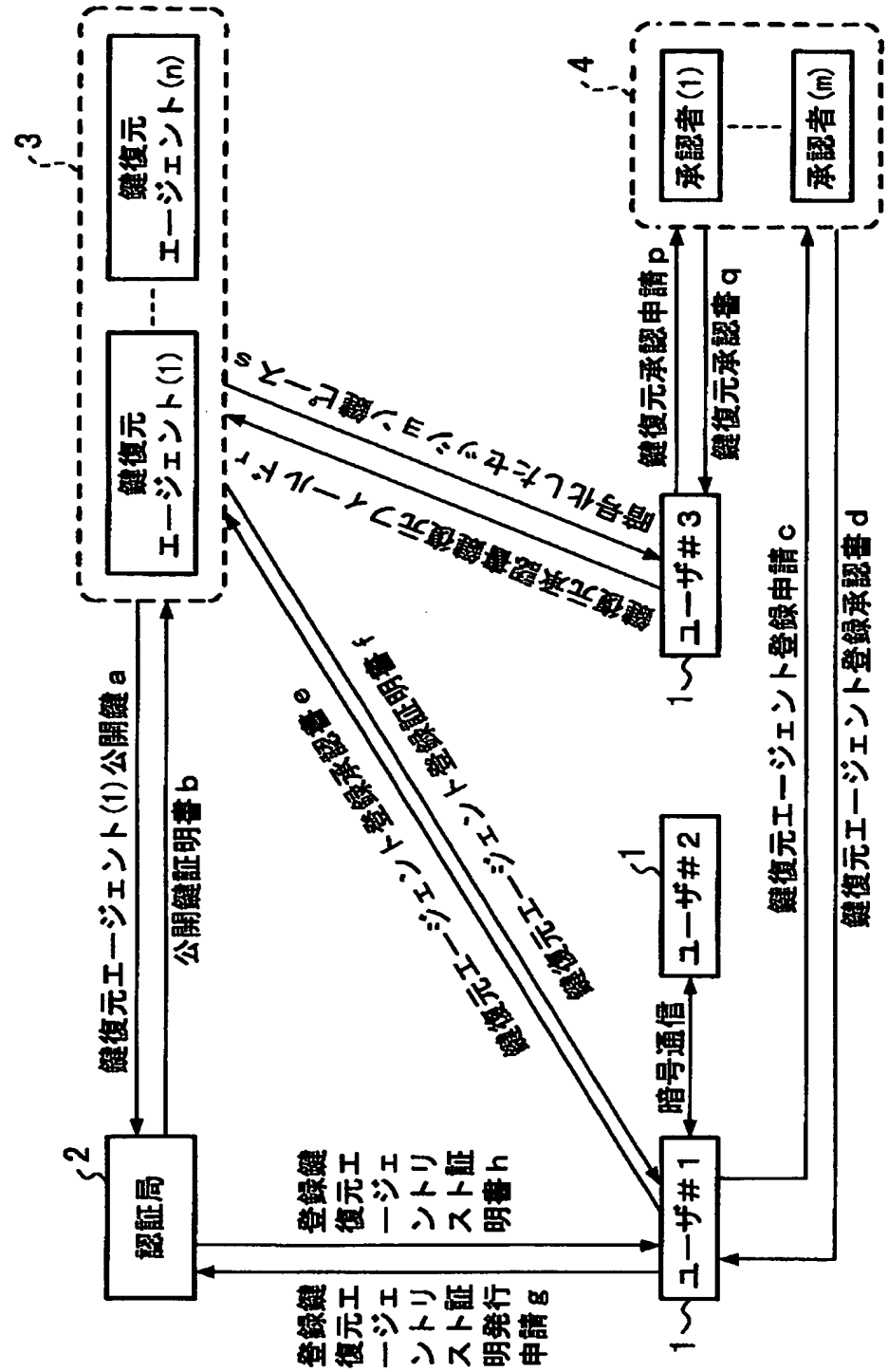
１７…キーボード

１８…プリンタ

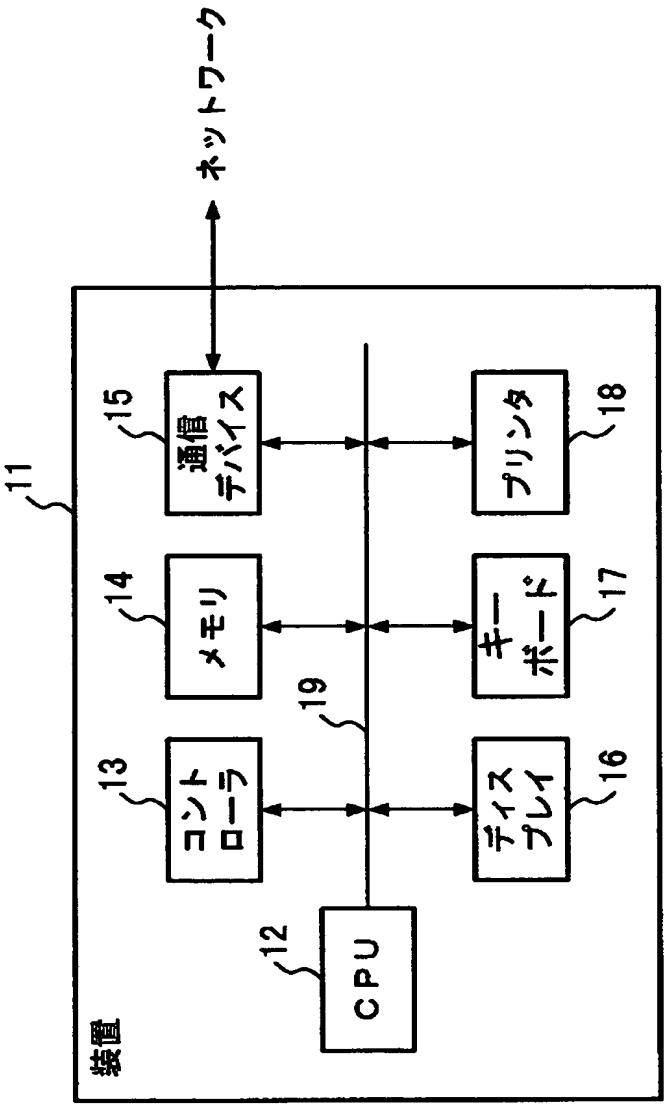
１９…データバス

【書類名】　　図面

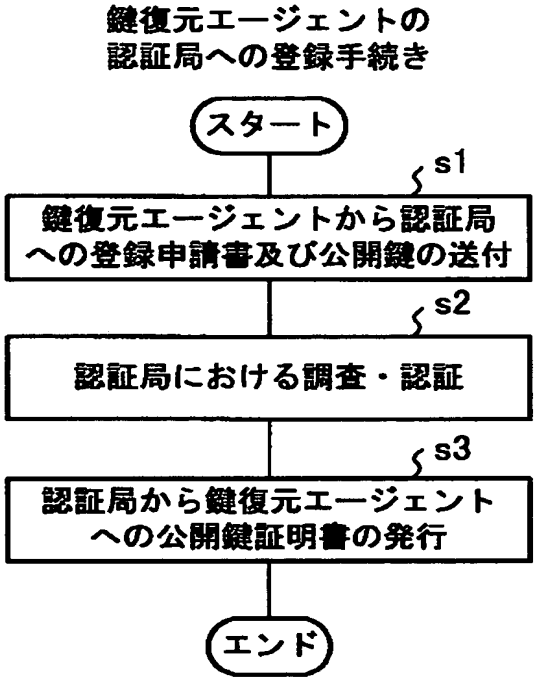
【図１】


3
鍵復元エージェント(n)
鍵復元エージェント(1)
4
承認者(1)
承認者(m)
暗号化したセッション鍵データ
鍵復元承認書鍵復元ファイル
鍵復元承認申請p
鍵復元承認書q
ユーザ#3
1
鍵復元エージェント(1)公開鍵a
公開鍵証明書b
鍵復元エージェント登録申請書c
鍵復元エージェント登録承認書d
鍵復元エージェント登録証明書f
鍵復元エージェント登録承認書e
ユーザ#2
1
暗号通信
2
認証局
登録鍵復元エージェントリスト証明書h
登録鍵復元エージェントリスト証明発行申請g
ユーザ#1
1

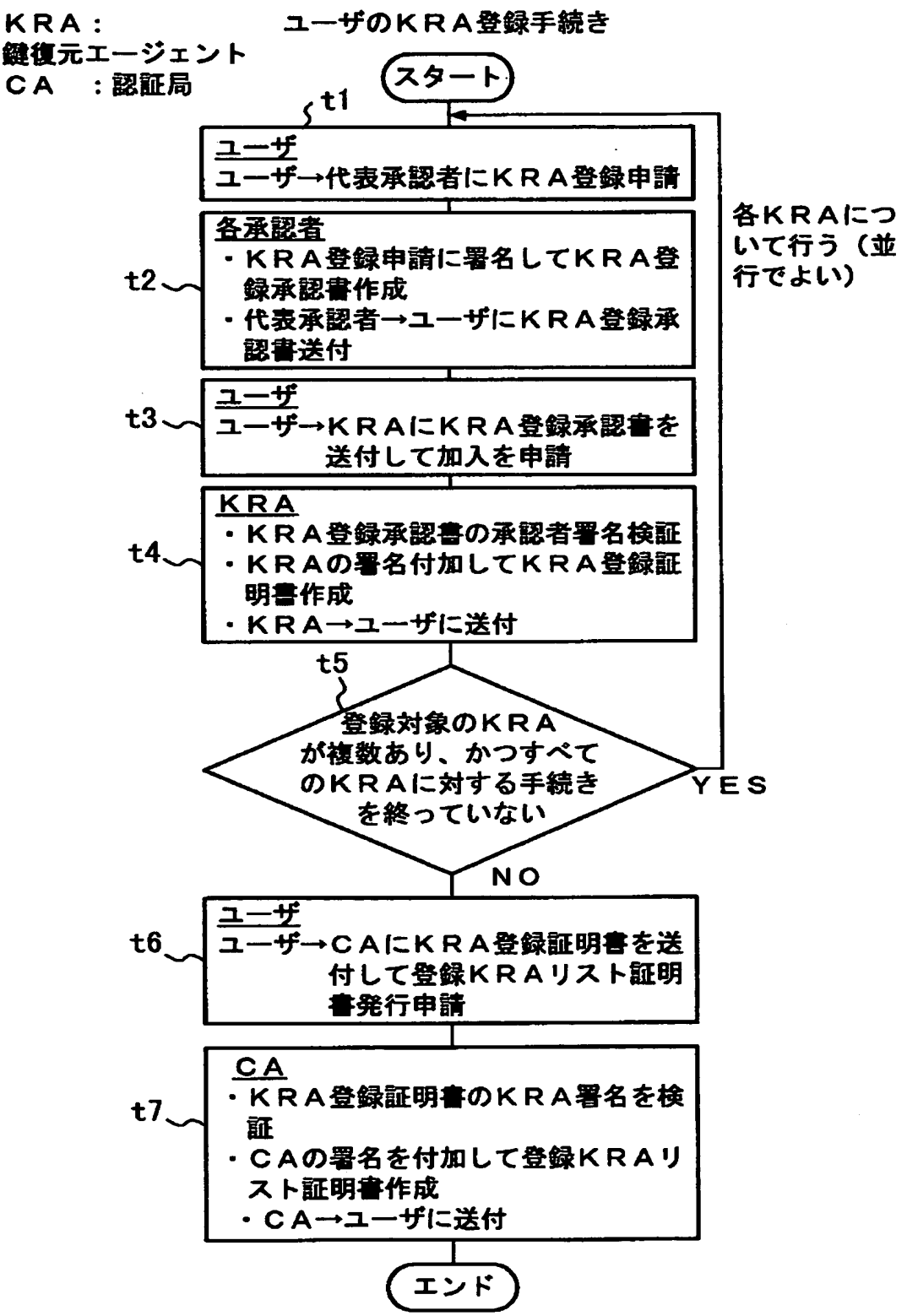
【図２】


ネットワーク
11
装置
12
CPU
13
コントローラ
14
メモリ
15
通信デバイス
16
ディスプレイ
17
キーボード
18
プリンタ
19

【図３】


鍵復元エージェントの
認証局への登録手続き
スタート
s1
鍵復元エージェントから認証局
への登録申請書及び公開鍵の送付
s2
認証局における調査・認証
s3
認証局から鍵復元エージェント
への公開鍵証明書の発行
エンド

【図４】

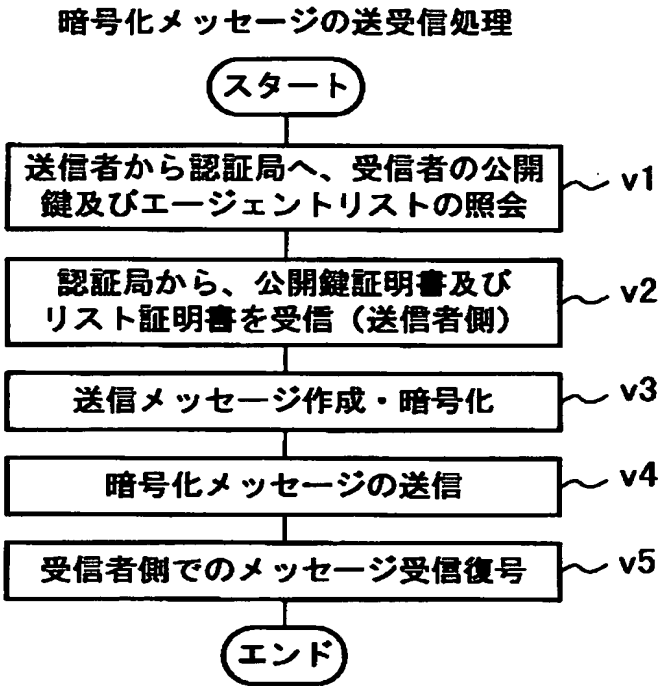

ＫＲＡ：
鍵復元エージェント
ＣＡ　：認証局
ユーザのＫＲＡ登録手続き
スタート
t1
ユーザ
ユーザ→代表承認者にＫＲＡ登録申請
各承認者
・ＫＲＡ登録申請に署名してＫＲＡ登録承認書作成
・代表承認者→ユーザにＫＲＡ登録承認書送付
t2
ユーザ
ユーザ→ＫＲＡにＫＲＡ登録承認書を送付して加入を申請
t3
ＫＲＡ
・ＫＲＡ登録承認書の承認者署名検証
・ＫＲＡの署名付加してＫＲＡ登録証明書作成
・ＫＲＡ→ユーザに送付
t4
t5
登録対象のＫＲＡが複数あり、かつすべてのＫＲＡに対する手続きを終っていない
ＹＥＳ
各ＫＲＡについて行う（並行でよい）
ＮＯ
ユーザ
ユーザ→ＣＡにＫＲＡ登録証明書を送付して登録ＫＲＡリスト証明書発行申請
t6
ＣＡ
・ＫＲＡ登録証明書のＫＲＡ署名を検証
・ＣＡの署名を付加して登録ＫＲＡリスト証明書作成
・ＣＡ→ユーザに送付
t7
エンド

【図５】

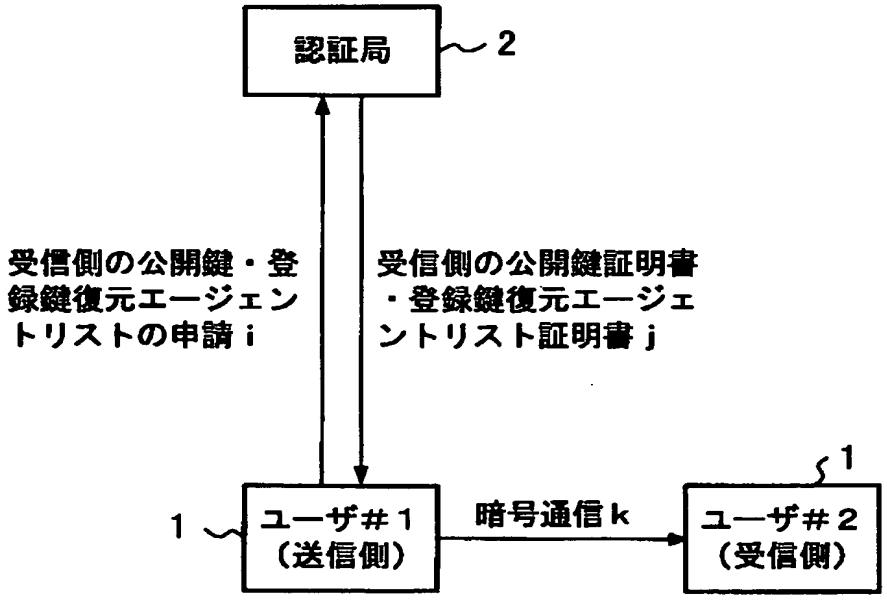
登録情報テーブル 21

ユーザ、承認者、鍵復元エージェントのＩＤ	認証局署名付公開鍵	ユーザが登録するエージェントリスト
ユーザ＃１	○○○○	A，B，C，
ユーザ＃２	××××	B，D，G，H
⋮	⋮	⋮
承認者α	△△△△	な　し
承認者β	□□□□	な　し
⋮	⋮	⋮
エージェントＡ	****	な　し
エージェントＢ	▽▽▽▽	な　し
⋮	⋮	⋮

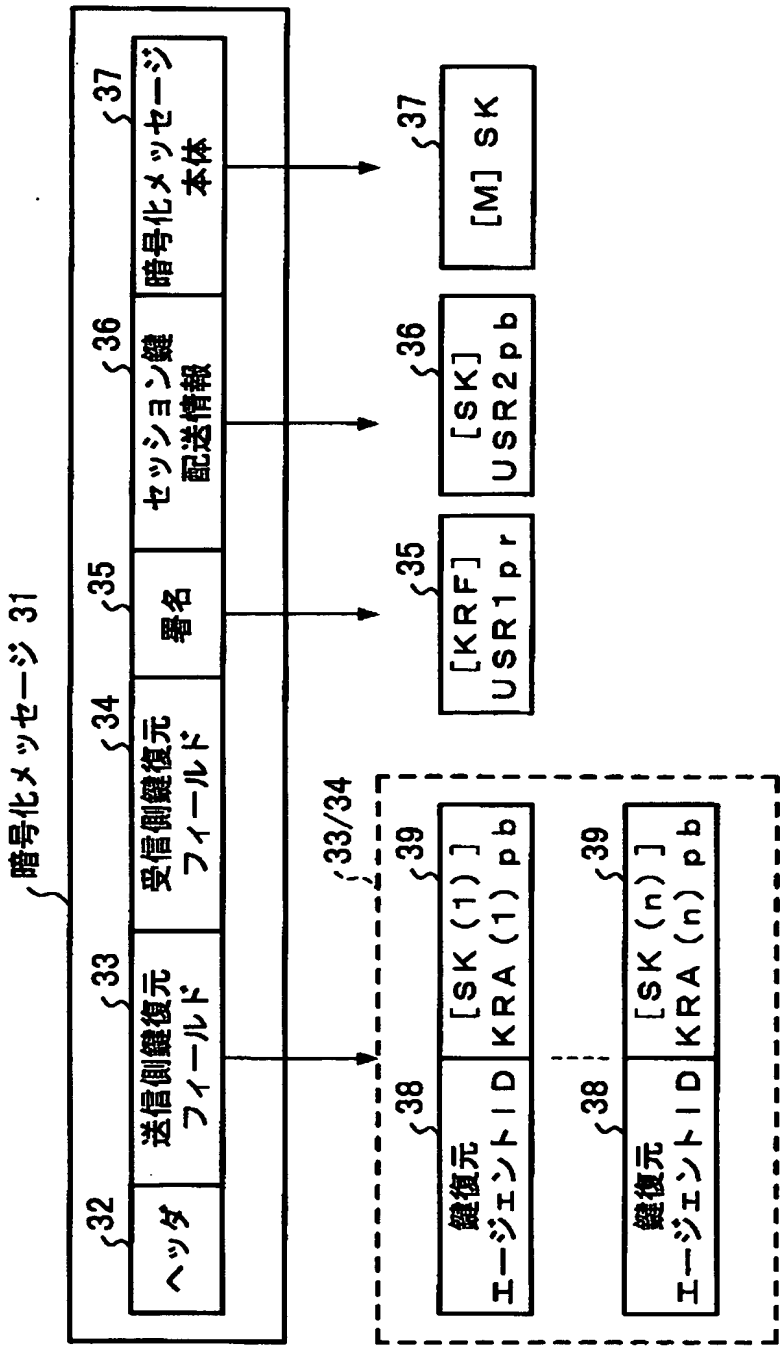
【図６】


暗号化メッセージの送受信処理
スタート
送信者から認証局へ、受信者の公開鍵及びエージェントリストの照会
v1
認証局から、公開鍵証明書及びリスト証明書を受信（送信者側）
v2
送信メッセージ作成・暗号化
v3
暗号化メッセージの送信
v4
受信者側でのメッセージ受信復号
v5
エンド

【図７】

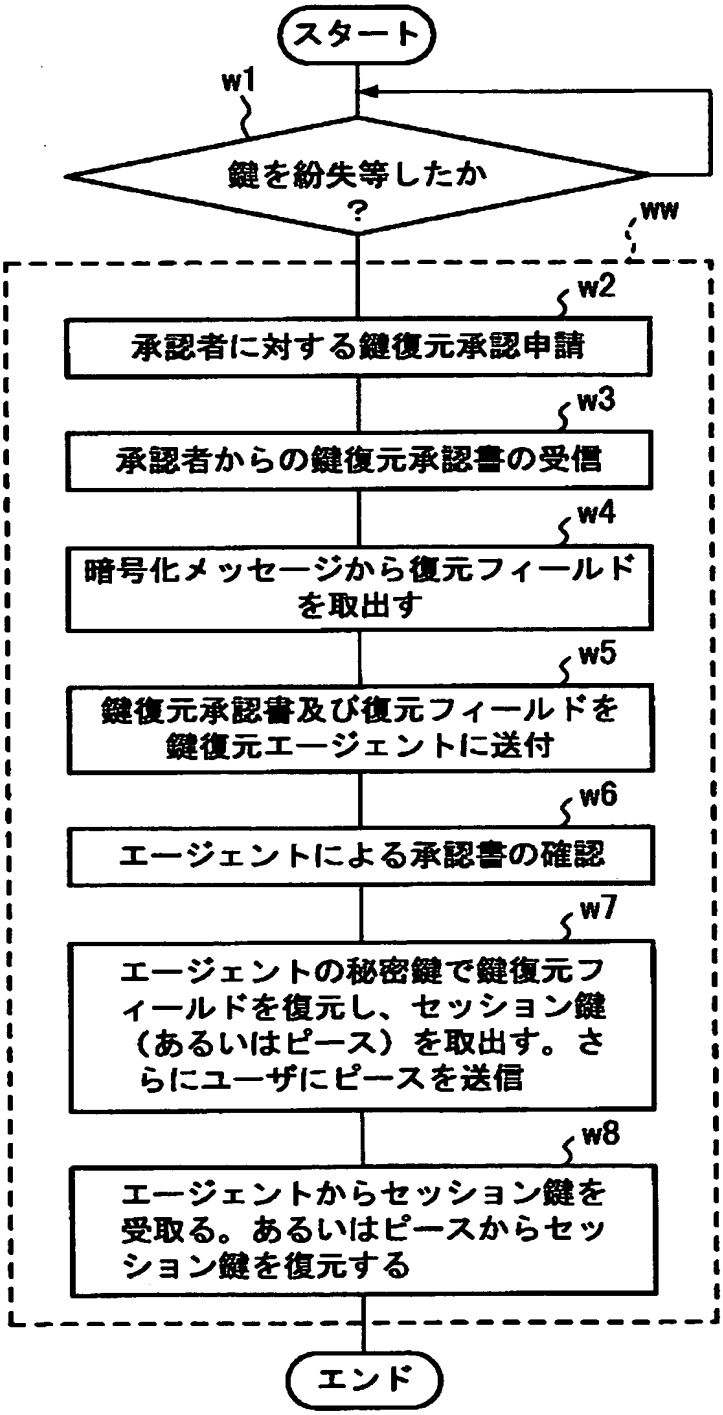

認証局
2
受信側の公開鍵・登録鍵復元エージェントリストの申請ｉ
受信側の公開鍵証明書・登録鍵復元エージェントリスト証明書ｊ
1
1
ユーザ＃１（送信側）
暗号通信ｋ
ユーザ＃２（受信側）

【図８】

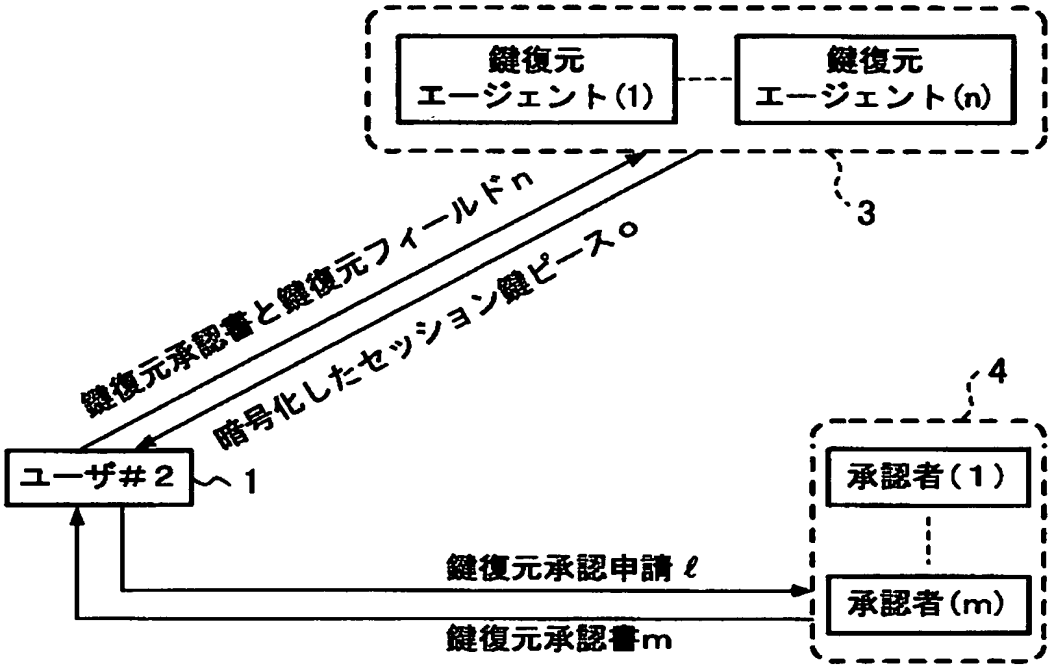

暗号化メッセージ 31
32
ヘッダ
33
送信側鍵復元フィールド
34
受信側鍵復元フィールド
35
署名
36
セッション鍵配送情報
37
暗号化メッセージ本体
33/34
38
鍵復元エージェントID
39
[SK(1)]KRA(1)pb
38
鍵復元エージェントID
39
[SK(n)]KRA(n)pb
35
[KRF]USR1pr
36
[SK]USR2pb
37
[M]SK

【図９】

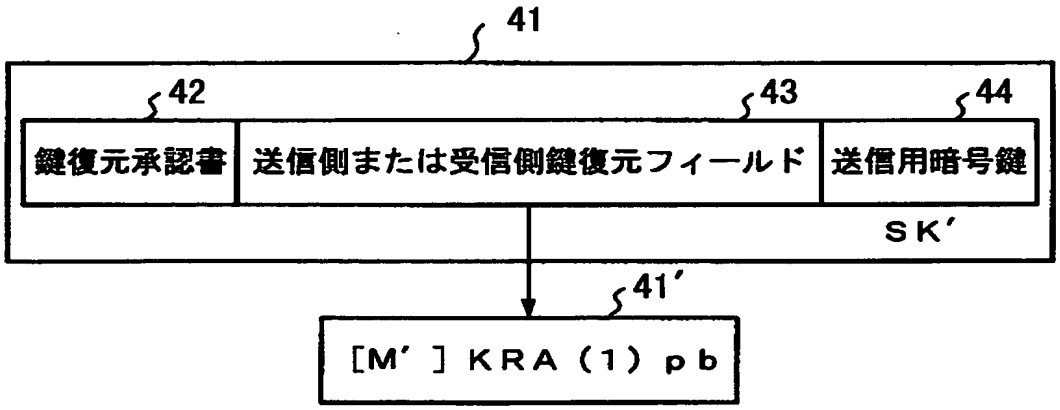
送信者又は受信者による鍵復元手続き



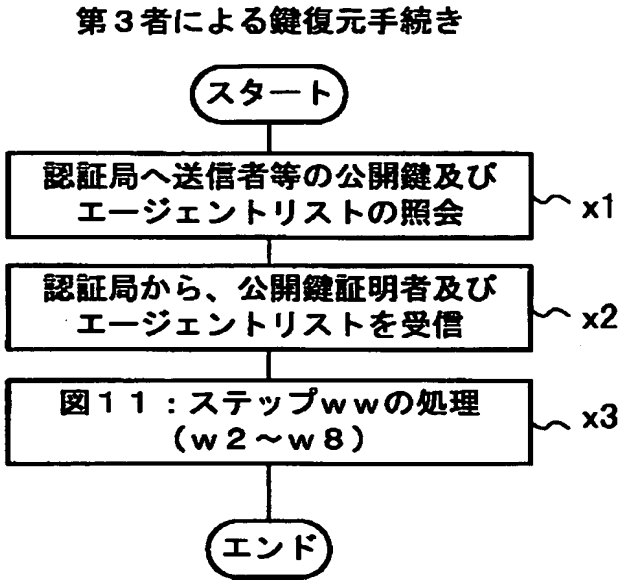
【図１０】


鍵復元
エージェント(1)
鍵復元
エージェント(n)
3
鍵復元承認書と鍵復元フィールドn
暗号化したセッション鍵ピースo
4
ユーザ＃２
1
承認者(1)
承認者(m)
鍵復元承認申請ℓ
鍵復元承認書m

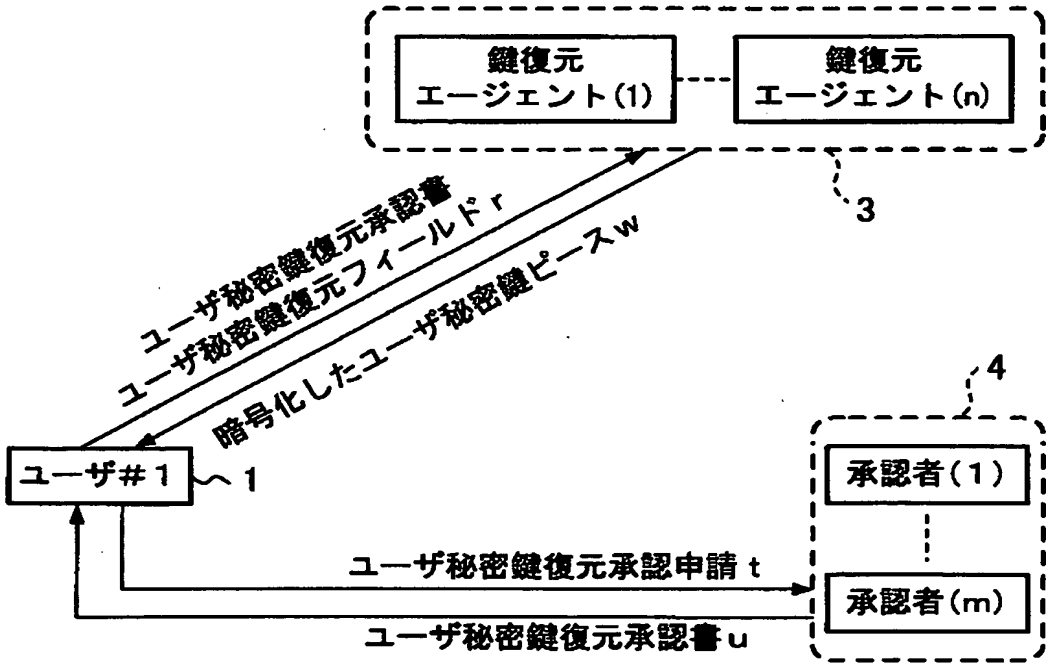
【図１１】


41
42
43
44
鍵復元承認書
送信側または受信側鍵復元フィールド
送信用暗号鍵
SK′
41′
[M′] KRA (1) pb

【図１２】


第３者による鍵復元手続き
スタート
認証局へ送信者等の公開鍵及び
エージェントリストの照会
x1
認証局から、公開鍵証明者及び
エージェントリストを受信
x2
図１１：ステップｗｗの処理
（ｗ２～ｗ８）
x3
エンド

【図１３】


鍵復元
エージェント(1)
鍵復元
エージェント(n)
3
ユーザ秘密鍵復元承認書
ユーザ秘密鍵復元フィールドr
暗号化したユーザ秘密鍵ピースw
4
ユーザ#１
1
承認者(1)
承認者(m)
ユーザ秘密鍵復元承認申請 t
ユーザ秘密鍵復元承認書u

【書類名】　　要約書

【要約】

【課題】　鍵復号に関する権限集中やエージェントの結託等の防止を可能として、鍵復元の安全性を高いものとすることができる。

【解決手段】　データ本体を暗号化して送信データ３１に含め、当該送信データを受信者に送信する暗号装置であって、暗号化したデータ本体３７を復号する鍵を復元するための復元用情報を、送信者が登録している鍵復元者に復号可能に暗号化した送信者鍵復元データ３３と、暗号化したデータ本体を復号する鍵を復元するための復元用情報を、受信者が登録している鍵復元者に復号可能に暗号化した受信者鍵復元データ３４とを送信データに含める手段１１を備えた暗号装置。

【選択図】　　図１

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000003078
【住所又は居所】　神奈川県川崎市幸区堀川町７２番地
【氏名又は名称】　株式会社東芝
【代理人】　申請人
【識別番号】　100058479
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　鈴江　武彦
【選任した代理人】
【識別番号】　100084618
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　村松　貞男
【選任した代理人】
【識別番号】　100068814
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　坪井　淳
【選任した代理人】
【識別番号】　100092196
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　橋本　良郎
【選任した代理人】
【識別番号】　100091351
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　河野　哲
【選任した代理人】
【識別番号】　100088683
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　中村　誠
【選任した代理人】

【識別番号】　100070437
【住所又は居所】　東京都千代田区霞が関３丁目７番２号　鈴榮内外國特許法律事務所内
【氏名又は名称】　河井　将次

出　願　人　履　歴　情　報

識別番号　　〔０００００３０７８〕

１．変更年月日　　１９９０年　８月２２日
［変更理由］　新規登録
住　所　神奈川県川崎市幸区堀川町７２番地
氏　名　株式会社東芝